Attorney Docket No. 1602.1007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Masahiro SAITO, et al.

Application No.: Group Art Unit:

Filed: January 28, 2002 Examiner:

For: SECURITY MANAGEMENT APPARATUS, SECURITY MANAGEMENT METHOD, AND SECURITY MANAGEMENT PROGRAM

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-293132

Filed: September 26, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 28, 2002 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　９月２６日

出願番号
Application Number: 特願２００１－２９３１３２

出願人
Applicant(s): 富士通株式会社

２００１年１１月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１０２３１６

【書類名】　特許願

【整理番号】　0150930

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

G01S 5/00

【発明の名称】　セキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラム

【請求項の数】　5

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　斉藤　優弘

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　木原　通三郎

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　大浦　滋明

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　水谷　佳代

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小野　仁子

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100097250

【弁理士】

【氏名又は名称】　石戸　久子

【選任した代理人】

【識別番号】　100101856

【弁理士】

【氏名又は名称】　赤澤　日出夫

【手数料の表示】

【予納台帳番号】　038760

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0014371

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラム

【特許請求の範囲】

【請求項１】　所定の装置のセキュリティを管理するセキュリティ管理装置であって、

前記所定の装置の位置を検出する位置検出手段と、

前記位置検出手段により検出された位置に応じてセキュリティレベルを変更する制御手段とを備えたことを特徴とするセキュリティ管理装置。

【請求項２】　所定の装置のセキュリティを管理するセキュリティ管理方法であって、

前記所定の装置の位置を検出する位置検出ステップと、

前記位置検出ステップにより検出された位置に応じてセキュリティレベルを変更する制御ステップとを備えたことを特徴とするセキュリティ管理方法。

【請求項３】　所定の装置のセキュリティを管理するセキュリティ管理用プログラムであって、

前記所定の装置の位置を検出する位置検出ステップと、

前記位置検出ステップにより検出された位置に応じてセキュリティレベルを変更する制御ステップとをコンピュータに実行させることを特徴とするセキュリティ管理用プログラム。

【請求項４】　所定の装置に格納されるプログラムであって、

前記所定の装置の位置が検出された場合、予め位置に対応付けられて記憶されたセキュリティレベルを、前記検出された位置に基づいて参照し、前記所定の装置のセキュリティ制御を行うことをコンピュータに実行させるプログラム。

【請求項５】　所定の装置のセキュリティを管理するための処理を実行するためのデータを記憶したコンピュータ読み取り可能なデータ記憶媒体であって、

位置とセキュリティレベルが対応付けられて記憶されており、前記セキュリティレベルは、前記所定の装置の検出位置に基づいて参照され、参照結果に基づいて前記所定の装置のセキュリティ制御が行われるための情報であることを特徴と

するコンピュータ読み取り可能なデータ記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、所定の装置のセキュリティを管理するセキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラムに関し、例えば、動作中の携帯型パーソナルコンピュータにおいて、ＯＳ等プログラムの起動やファイルへのアクセスについてのセキュリティ制御を、該携帯型パーソナルコンピュータの位置に応じて行うセキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラムに関するものである。

【０００２】

【従来の技術】

一般的なコンピュータでは、ＢＩＯＳがＯＳの起動時にユーザにパスワードを要求し、入力されたパスワードにより、ＯＳの起動を制限してセキュリティを保護する機能が備えられている。また、ＯＳへのログイン時にユーザに対しパスワードを要求し、入力されたパスワードにより、ＯＳへのログインを制限したり、また、ファイルに対して予めアクセス権を設定しておき、ログインしたユーザの権限によりファイルへのアクセスを制限することができる機能が備えられている。

【０００３】

【発明が解決しようとする課題】

しかしながら、このような従来の技術においては、例えば携帯型パーソナルコンピュータのＯＳの起動後は、ログインしたユーザがログオフするまでの間、そのユーザの権限に応じてファイルのアクセスが可能となるため、例えばログインした状態で携帯型パーソナルコンピュータが盗難に遭った場合には、ファイルにアクセス制限が設定されている場合であっても、そのファイルに不正にアクセスされてしまうという問題が生じる。また、ファイルに対するアクセス権を持つユーザが携帯型パーソナルコンピュータにログインし、使用する場合であっても、通勤中の電車内等で使用する場合は、誤って機密事項等を有するファイルを開い

てしまい、それを第三者に見られ、機密情報が漏洩するという恐れがある。

【０００４】

このような問題を回避するために、従来は、携帯型パーソナルコンピュータの使用を中断し席を外す場合等には、そのパーソナルコンピュータの電源を切る、あるいはＯＳを終了させ再起動する、あるいはログオフして再ログインする等して、第三者の不正アクセスを防止するようにしていた。また、使用場所が移る場合も同様に、再ログイン等の処理を行っていた。しかしながら、このような処理をユーザがいちいち行うのは非常に面倒であり、手間がかかる。また、セキュリティ制御がユーザまかせになり、セキュリティ管理が甘くなる。

【０００５】

本発明は、そのような問題を解決するためになされたもので、ＯＳの起動やファイルに対してアクセスする権限を、携帯型パーソナルコンピュータが動作している位置によって変えることで、例えば会社内等の特定の範囲内でのみＯＳの起動やファイルへのアクセスをできるようにし、セキュリティ機能の向上を図るとともに、従来、使用場所が移動する度に行われていたＯＳ再起動、再ログインといったユーザの作業を軽減させることのできるセキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラムを提供することを目的としている。

【０００６】

【課題を解決するための手段】

上述した課題を解決するため、本発明は、所定の装置のセキュリティを管理するセキュリティ管理装置であって、前記所定の装置の位置を検出する位置検出手段と、前記位置検出手段により検出された位置に応じてセキュリティレベルを変更する制御手段とを備えたことを特徴とするものである。

【０００７】

このような構成によれば、特定のエリアでのみ、所定の装置、例えば携帯型パーソナルコンピュータ等の、ＯＳの起動やファイルのアクセスを可能とすることができ、また、特定のエリアの外に移動した場合は、ＯＳの起動やファイルのアクセスを不可とすることができる。従って、セキュリティ機能が向上する。本発

明の実施の形態において、上述の位置検出手段は、位置検出部に相当する。なお、位置を検出するための技術はＧＰＳやＰＨＳにおける位置検出機能であってもよく、特に限定しない。さらに、セキュリティレベルは本実施の形態ではアクセス権の種類に相当する。さらにまた、制御手段は、制御部及びセキュリティ設定切替え部により構成される。

【０００８】

また、前記セキュリティレベルを位置に対応付けて記憶するセキュリティ情報記憶手段を備え、前記制御手段は前記位置検出手段により検出された位置に基づいて、前記セキュリティ情報記憶手段に記憶されたセキュリティレベルに変更するようにしてもよい。このようにセキュリティレベルを位置に対応付けて記憶させておけば、該記憶された情報に基づいて自由にセキュリティレベルを変更することができ、また該変更処理を容易に行うことができる。

【０００９】

また、前記セキュリティレベルはさらにユーザに対応付けられて前記セキュリティ情報記憶手段に記憶され、前記制御手段は前記位置検出手段により検出された位置と前記ユーザとに基づいて、前記セキュリティ情報記憶手段に記憶されたセキュリティレベルに変更するようにすることもできる。本発明の実施の形態においては、セキュリティ情報テーブルに位置とユーザに対応したグループ名が記憶されており、セキュリティ設定切替え部がセキュリティ情報テーブルを参照して位置とユーザ名に基づいて当該ユーザの所属するグループ名を取得し、設定する。ＯＳはアクセス権設定テーブルを参照して設定されているグループ名に基づいてアクセス権の種類を取得し、取得したアクセス権に基づいてセキュリティ制御を行う。このように位置及びユーザによってセキュリティ管理を行えば、セキュリティ機能が向上し、細やかな制御が可能となる。

【００１０】

さらに、本発明に係るセキュリティ管理装置において、前記ユーザをユーザ識別子として入力設定することができるログイン機能を備えるようにしてもよい。

【００１１】

このような構成によれば、所定の装置を使用するユーザが複数存在している場

合でも、ユーザ毎に細やかなセキュリティ制御を行うことができる。なお、本発明の実施の形態において、ログイン機能により入力設定されるユーザ識別子は、ユーザ名に相当し、セキュリティ管理の対象である動作中の装置において、位置が検出された場合、セキュリティ情報テーブルから検出された位置及びログイン時のユーザ名によって当該ユーザが所属するグループ名が特定され、そのグループ名によって様々なセキュリティ制御を行う。

【００１２】

さらに、本発明に係るセキュリティ管理装置において、前記セキュリティ情報記憶手段に記憶される情報を入力し、又は前記セキュリティ情報記憶手段に記憶された内容を変更又は削除するためのセキュリティ情報設定手段を備えるようにすることもできる。

【００１３】

このような構成によれば、セキュリティレベルを自由に設定することが可能となるため、セキュリティレベルを所定の装置の使用状況や使用する地域等に対応させることができ、ユーザの希望を満たす細やかなセキュリティ制御を行うことができるようになる。なお、本発明の実施の形態において、セキュリティレベルについての情報を記憶したセキュリティ情報テーブル及びアクセス権設定テーブルのうち、セキュリティ情報テーブルは、ＧＰＳ対応の地図を用いて、設定を希望する範囲をユーザがマウスなどにより選択することによって経度及び緯度を特定し、特定したエリアに対してグループ名を入力・変更・削除できるようにしている。また、アクセス権設定テーブルに対しては、希望するファイルやプログラムのアクセス権をグループ名毎に入力したり、変更や削除などができるようにしている。このような処理はテーブル入力部により行われる。

【００１４】

また、本発明に係るセキュリティ管理装置において、前記セキュリティレベルには、前記制御手段によりセキュリティ制御が行われる対象と、その制御内容が規定されるようにしてもよい。さらに、本発明に係るセキュリティ管理装置において、前記セキュリティ制御が行われる対象は、前記所定の装置が扱うファイルもしくはフォルダもしくはディレクトリもしくはプログラムの少なくともいずれ

かとすることができる。さらにまた、本発明に係るセキュリティ管理装置において、前記対象についての制御内容はアクセス権の種類とすることができる。

【００１５】

このような構成によれば、例えば携帯型パーソナルコンピュータにおいて通常頻繁にアクセスされるファイルやフォルダ、ディレクトリやプログラムに対して、例えば、読み取り専用、変更可能、アクセス不可等、アクセス権の種類を細やかに設定することができ、セキュリティを強化することができる。

【００１６】

さらに、本発明に係るセキュリティ管理装置は、前記所定の装置内に設けられていてもよい。このようにセキュリティ管理装置がセキュリティ管理の対象である所定の装置内にあれば、セキュリティの制御が容易になる。

【００１７】

さらに、本発明に係るセキュリティ管理装置において、前記制御手段はＯＳで構成され、前記所定の装置はパーソナルコンピュータとすることができる。このような構成によれば、広く一般的に使用されるコンピュータに対し、追加的に特別なハードウェアを備えることなく、優れたセキュリティ管理を容易に行うことができる。

【００１８】

また、本発明は、所定の装置のセキュリティを管理するセキュリティ管理方法であって、前記所定の装置の位置を検出する位置検出ステップと、前記位置検出ステップにより検出された位置に応じてセキュリティレベルを変更する制御ステップとを備えたことを特徴とするものである。

【００１９】

また、本発明は、上述した方法をコンピュータに実行させるためのプログラムを提供する。さらに、上述した制御ステップをＯＳが行うようにすれば、それ以外のステップを実行するための容量の小さいアプリケーションをインストールするだけでコンピュータに位置によるセキュリティ管理を容易に実行させることができる。

【００２０】

また、本発明は、上述したセキュリティ管理を実行するために、位置とセキュリティレベルが対応づけられて記憶したコンピュータ読み取り可能なデータ記憶媒体を提供する。このようなデータ記憶媒体をＯＳが参照可能な状態でコンピュータに格納すれば、セキュリティ管理を容易に実行させることができる。また、記録されたデータが可変であれば、使い勝手よくセキュリティ管理を行うことができる。さらに、このようなデータを入力、削除、変更することができるプログラムをコンピュータに格納しておけば、さらにユーザの使い勝手がよくなる。

【００２１】

【発明の実施の形態】

以下、図を用いて、本発明の実施の形態を詳細に説明する。

図１は、本発明に係るセキュリティ管理装置の基本構成を簡略的に示したブロック図である。本実施の形態において、セキュリティ管理装置は、管理対象となる装置（本例ではセキュリティ管理装置自身）の位置を検出し、検出された位置によってセキュリティ管理装置内の様々な対象（ファイルやフォルダなど）へのアクセス権の制御を行う。

【００２２】

図において、セキュリティ管理装置１０（以下、装置１０）は、無線による通信を行う無線通信部１１と、無線通信で取得した情報から装置１０の現在位置を検出する位置検出部１２と、装置１０の起動時のログイン制御や、各種入出力の制御を行う入出力制御部１３、位置及びユーザ名とそれらに対応するセキュリティ関連情報が格納されたセキュリティ情報テーブル１４、ファイルやフォルダ、プログラム等とその各々に対応するアクセス権の情報が格納されたアクセス権設定テーブル１５、セキュリティ情報テーブル１４から現在位置に対応するセキュリティ関連情報を検索し、セキュリティ設定の切り替えを行うためのセキュリティ設定切替え部１６、セキュリティ情報テーブル１４とアクセス権設定テーブル１５に対する入力及び編集を行うテーブル入力部１７、装置１０全体の機能を制御し、セキュリティ設定切替え部１６によるセキュリティ設定に基づいてプログラムやファイルに対するアクセス制御を行う制御部１８からなる。

【００２３】

図２は、図１に示された装置１０が適用される携帯型パーソナルコンピュータ２０の構成例であり、ノースブリッジ２１と、このノースブリッジ２１に接続されたＣＰＵ２２とメモリ２３を備える。また、ノースブリッジ２１に接続されたサウスブリッジ２４と、サウスブリッジ２４に接続され、ＢＩＯＳを格納したＢＩＯＳ用ＲＯＭ２５と、キーボードコントローラ２６、及びこれに接続されたキーボード２７とマウス２８、Ｉ／Ｏコントローラ２９、及びこれに接続されたシリアルポート３０、パラレルポート３１、ＦＤＤ３２、電源ユニット３３とを備えている。なお、シリアルポート３０及びパラレルポート３１には、それぞれに対応したインターフェースを備えるデバイスを接続可能である。

【００２４】

さらに、本携帯型パーソナルコンピュータ２０は、ディスプレイコントローラ３４、及びこれに接続されたＬＣＤ３５、位置検出手段としてのＧＰＳ３６、及びこれに接続され衛生から電波を受信するアンテナ３７、ディスクコントローラ３８、及びこれに接続されたＨＤＤ３９とを備えている。

【００２５】

以上の構成において、図１に示された無線通信部１１は、図２においては主としてアンテナ３７及びＧＰＳ３６により構成され、位置検出部１２は主としてＧＰＳ３６により構成される。また、図１の入出力制御部１３は、図２のＨＤＤ３９に格納されたＯＳにより構成される。さらに、図１の制御部１８は図２のＣＰＵ２２により構成され、本発明を実施する際にはＨＤＤ３９に格納された本発明を実施するための特定のアプリケーション（以下、アプリケーション）及びＯＳによる各種制御処理等を実行する。また、セキュリティ設定切替え部１６及びテーブル入力部１７は、当該アプリケーションの制御機能とは別に当該アプリケーションに備えられた設定機能の一部である。

【００２６】

上述の構成による本実施の形態の動作を簡単に説明する。制御部１８は、位置検出部１２に対し、現在位置を取得するための制御信号を定期的に出力する。制御部１８から制御信号を受信した位置検出部１２は無線通信部１１により受信した無線情報から現在位置の情報を検出する。なお、位置の検出は図２に示される

ようにＧＰＳの技術を用いてもよいし、ＰＨＳや携帯電話などの位置情報サービスの技術を使用してもよい。このような位置情報サービスの技術を使用する場合には、図２のＧＰＳ３６及びアンテナ３７に代えて、このサービスを利用しうるＰＨＳや携帯電話を用いる。なお、これらＰＨＳ、携帯電話はコンピュータに内蔵されたものでもよいし、ケーブルでコンピュータに接続されたものでもよい。本発明の位置検出においては、システム種別もしくはデバイス種別を特に限定するものではない。

【００２７】

こうして無線情報から現在位置の情報を検出した位置検出部１２は、当該位置の情報を制御部１８を介してセキュリティ設定切替え部１６に受け渡す。位置検出部１２から現在位置の情報を取得したセキュリティ設定切替え部１６は、セキュリティ情報テーブル１４を参照し、そこから現在位置に対応したセキュリティ関連情報を取得する。なお、セキュリティ情報テーブル１４は、図２のディスクコントローラ３８により制御されるＨＤＤ３９が保持する。図３はセキュリティ情報テーブル１４の一例である。本実施の形態において、セキュリティ設定切替え部１６が取得するセキュリティ関連情報は、「位置の範囲」と「ユーザ名」から特定される「ユーザの所属するグループ名」（以下、グループ名）である。なお、本実施の形態において、現在位置及びログインしたユーザ名によりセキュリティ情報テーブル１４に該当のグループ名が存在しない場合には、装置の電源が切断される。セキュリティ情報テーブル１４は、後述するようにユーザにより入力・編集が可能である。

【００２８】

セキュリティ設定切替え部１６は、セキュリティ情報テーブル１４から取得したグループ名を当該携帯型パーソナルコンピュータ２０を使用するユーザのセキュリティ設定値として保持し、制御部１８は、当該設定値を基にアクセス権設定テーブル１５を参照し、そこから当該設定値に対応したアクセス権の情報を取得して、ファイルやプログラムなどのアクセス制御を行う。なお、アクセス権設定テーブル１５は、図２のディスクコントローラ３８により制御されるＨＤＤ３９が保持する。図４はアクセス権設定テーブル１５の一例である。本実施の形態に

おいて、制御部１８は、ファイルやプログラムに対してアクセス命令が出されると、設定値として保持されている「グループ名」から該当する「アクセス権の種類」を参照し、その「アクセス権の種類」に応じて、アクセス命令の出されたファイルやプログラムに対するセキュリティ管理を行う。

【００２９】

図５及び図６は本発明のセキュリティ設定の変更及びアクセス制御を含むセキュリティ管理のフローチャートである。これらの図を用いて、本実施の形態におけるセキュリティ管理の処理を詳細に説明する。なお、ここでは制御部１８による処理を、ＯＳによる処理とアプリケーションによる処理とに分けて説明する。

【００３０】

まず、ユーザが装置の電源を入れる（Ｓ５０）。ＯＳが起動し、ユーザがＯＳにログインする（Ｓ５１）。このログイン制御は入出力制御部１３（ＯＳ）により行われ、ユーザ名を入力するためのログイン画面を表示する。そして、ユーザにより入力されたユーザ名を用いてログイン認証処理を実行する。ただし、ここでログインが完了してもユーザが使用できる状態とはならない。ログイン後、位置検出部１２により現在の位置を検出する（Ｓ５２）。なお、本実施の形態では、位置の検出は、アプリケーションにより定期的（等間隔、ログイン直後、Ｒｅｓｕｍｅ直後など）に行うようにしている。

【００３１】

次に、セキュリティ設定切替え部１６は、検出された現在位置がセキュリティ情報テーブル１４に存在するかどうか、及び、同一レコード内にログインしたユーザのユーザ名が存在するかどうかの参照を行う（Ｓ５３）。セキュリティ情報テーブル１４内に、該当する「位置の範囲」とログインしたユーザの「ユーザ名」が記録されたレコードが存在しない場合は（Ｓ５４、ＮＯ）、アプリケーションは電源切断のメッセージを表示し（Ｓ５５）、電源切断を行う（Ｓ５６）。図７は電源切断時に表示されるポップアップメッセージの例である。ポップアップ画面中の［ＯＫ］ボタンがユーザによりクリックされると、アプリケーションは、ＯＳの終了処理を行う。

【００３２】

セキュリティ情報テーブル１４内に、該当する「位置の範囲」とログインしたユーザの「ユーザ名」が記録されたレコードが存在する場合は（Ｓ５４、ＹＥＳ）、セキュリティ設定切替え部１６は「位置の範囲」と「ユーザ名」に対応する「ユーザの所属するグループ名」（グループ名）を取得する。ここで、装置１０が起動直後の場合には（Ｓ５７、起動時設定）、ユーザの所属するグループ名は未設定状態であるため、取得されたグループ名が即座に設定値とされる（Ｓ６２）。設定されると装置１０は使用可能な状態となる。

【００３３】

グループ名の設定後は、アクセス権設定テーブル１５に基づいてアクセス制御を行う。図６において、ユーザからファイルオープン命令があった場合（Ｓ６３、ＹＥＳ）、ＯＳはアクセス権設定テーブル１５を参照し、該当のファイルのアクセス権の種類を確認する（Ｓ６４）。アクセス権の種類が「アクセス不可」である場合（Ｓ６４、アクセス不可）、ＯＳはアクセス不可である旨のメッセージを表示し、ファイルをオープンしない（Ｓ６５）。アクセス権の種類が「読み取り可能」である場合（Ｓ６４、読み取り可能）、ＯＳはアクセス権がファイルを編集できない読み取り専用である旨のメッセージを表示し、読み取り専用でファイルをオープンする（Ｓ６６）。アクセス権の種類が「編集可能」である場合（Ｓ６４、フルアクセス）、ＯＳは読み書き自由のフルアクセスとしてファイルをオープンする（Ｓ６７）。なお、ファイルではなくフォルダやディレクトリであっても、ファイルと同様にアクセス権設定テーブル１５にアクセス権の種類を予め設定しておけば、アクセス制御は可能である。

【００３４】

ユーザからの命令がファイルオープン命令ではなく（Ｓ６３、ＮＯ）、プログラムの起動命令であった場合（Ｓ６８、ＹＥＳ）、ＯＳはアクセス権設定テーブル１５を参照し、該当のプログラムのアクセス権の種類を確認する（Ｓ６９）。アクセス権の種類が「起動不可」である場合（Ｓ６９、起動不可）、ＯＳはアクセス不可である旨のメッセージを表示し、プログラムを起動しない（Ｓ７０）。アクセス権の種類が「起動可」である場合（Ｓ６９、起動可）、プログラムを起動する（Ｓ７１）。

【００３５】

上述のアクセス制御とは別に、本実施の形態では位置検出の制御も行われる。アプリケーションにより予め定められた時刻となった場合（Ｓ７２、ＹＥＳ）、図５のＳ５２の処理に戻って現在位置の検出を行う。そうでなければ（Ｓ７２、ＮＯ）、Ｓ６３の処理に戻る。本実施の形態では、位置検出を定期的（等間隔、ログイン直後、Ｒｅｓｕｍｅ直後など）に行うようにしており、その検出間隔やタイミングはアプリケーションにより設定が可能である。

【００３６】

ここで、位置検出の結果、ユーザが装置１０を使用中に、現在位置がセキュリティ情報テーブル１４内に存在しない位置範囲に移動してしまった場合には（Ｓ５４、ＮＯ）、上述と同様Ｓ５５、Ｓ５６の電源切断処理が行われる。但し、この時、エディタ等で編集中のファイルがある場合は、エディタの機能によりファイルを保存するか否かのポップアップウィンドウが表示され、ユーザはその機能により、電源切断前に保存等の処理を実行することが可能である。

【００３７】

また、移動によりグループ名設定を変更する必要が生じた場合（Ｓ５７、変更要）、セキュリティ設定切替え部１６はグループ名変更によりアクセス権が変更される旨のメッセージを表示する（Ｓ５８）。図８はグループ名の設定変更処理時に表示されるポップアップメッセージの例である。ポップアップ画面中の［ＯＫ］ボタンがユーザによりクリックされると、セキュリティ設定切替え部１６は、実行中のファイルやプログラムがある場合には（Ｓ５９、ＹＥＳ）、ＯＳは実行中のファイル／プログラムのアクセス権をアクセス権設定テーブル１５により確認し、変更後のグループ名のアクセス権が変更前のグループ名のアクセス権の下位に属する場合は（Ｓ６０、ＹＥＳ）、それらのファイル／プログラムの終了処理を行う（Ｓ６１）。ここで、エディタ等で編集中のファイルがある場合は、エディタの機能によりファイルを保存するか否かのポップアップウィンドウが表示され（図示せず）、ユーザはその機能により、電源切断前に保存等の処理を実行することが可能である。

【００３８】

その後、セキュリティ設定切替え部１６は、ユーザの所属するグループ名の設定を変更し（Ｓ６２）、ＯＳはその変更に基づいてＳ６３からＳ７１のようにアクセス制御を行う。

【００３９】

なお、グループ名設定変更時にファイルやプログラムを実行中でない場合には（Ｓ５９、ＮＯ）、アクセス権のチェックは行われず、即座に設定変更（Ｓ６２）が行われる。また、ファイルやプログラムが実行中であっても、変更後のアクセス権が変更前のアクセス権の下位に属さない場合には（Ｓ６０、ＮＯ）、実行中のファイルやプログラムは終了せず、グループ名設定変更（Ｓ６２）のみが行われるため、作業を続行することができる。

【００４０】

次に、アプリケーションによりセキュリティ情報テーブル１４及びアクセス権設定テーブル１５に対する入力処理及びそれに伴うアクセス制御の詳細を図９及び図１０を用いて具体的に説明する。本実施の形態では、ユーザ（Ｕｓｅｒ１）が、会社、通勤経路、自宅のそれぞれの位置範囲を指定してそれぞれグループ名を設定し、セキュリティ制御を行うものとする。図９は、セキュリティ情報テーブル１４の位置とユーザ名とグループ名の入力画面例である。また、図１０は、図９に示されるセキュリティ情報テーブル１４の入力画面にて入力される会社、通勤経路、自宅の位置範囲の経度及び緯度を示した図である。

【００４１】

まず、ユーザ（Ｕｓｅｒ１）は、予めアプリケーションの機能の一部、テーブル入力部１７を使用し、図９に示されるような入力画面を表示させて、位置の範囲、ユーザ名、ユーザの所属するグループ名の設定を行う。本実施の形態では、図中においてユーザ名９０及びユーザの所属するグループ名９１を入力し、画面に表示された地図９２の中で設定する位置の範囲９３をマウスにより選択し、［保存］ボタン９４をクリックすることによって、設定の追加を行う。

【００４２】

図に従って説明すると、Ｕｓｅｒ１が、Ｕｓｅｒ１の会社、通勤経路、自宅のそれぞれの位置の範囲として、図１０に示されるように選択した場合、それぞれ

の選択された位置の範囲は、会社が、Ａ＜緯度＜Ｂ、Ｃ＜経度＜Ｄ、通勤経路がＥ＜緯度＜Ｆ、Ｄ＜経度＜Ｇ、自宅が、Ｈ＜緯度＜Ｉ、Ｇ＜経度＜Ｊとなり、それぞれの位置の範囲に対し、ユーザ名とユーザの所属するグループ名を入力して保存する。例えば、Ｕｓｅｒ１は会社及び自宅では、Ａｄｍｉｎｉｓｔｒａｔｏｒｓのグループに所属し、通勤経路では、Ｕｓｅｒｓのグループに所属する様に設定を行うようにすれば、会社及び自宅のアクセス制御と通勤経路のアクセス制御を区別して行うことができる。なお、［削除］ボタン９５により上述の設定を削除することも可能である。入力設定されると、現在の設定９７の一覧に追加され表示される。

【００４３】

本画面を終了させると、入力されたデータが図３に示されるセキュリティ情報テーブル１４に反映される。ここでは、Ｕｓｅｒ１の場合、会社がレコードＮｏ．１、通勤経路がレコードＮｏ．３、自宅がレコードＮｏ．５に該当する。また、セキュリティ情報テーブル１４は、ユーザ単位で設定することができ、それにより、複数のユーザによって１つの携帯型パーソナルコンピュータが使用される場合であっても、各ユーザの使用状況に応じて、位置によるセキュリティ設定を行うことができる。なお、図９において、［変更］ボタン９６をクリックすることによって、既に入力済みの各レコードを変更することも可能である。

【００４４】

アクセス権設定テーブル１５は、本実施の形態では、ＯＳの機能により設定入力されるものとする。本実施の形態では、自宅及び会社では、機密事項等を有するファイルやフォルダに読み書き自由でアクセスすることができ、通勤経路では、ファイルやフォルダにアクセスできない様に設定する。設定入力の画面の図示は省略する。設定入力の結果は、図４に示されるとおりである。図４はファイルやフォルダのアクセス権の設定例であり、ユーザの所属するグループ名により、アクセス不可／読み取り可能／変更可能等に設定されている。

【００４５】

図に示されるように、設定値（グループ名）がＡｄｍｉｎｉｓｔｒａｔｏｒｓの場合には、［Ｃ：￥ＤＯＣ￥機密事項］、［Ｃ：￥ＤＯＣ￥公開情報］の両方

のフォルダに読み書き自由でアクセス可能（アクセス権の種類：「変更可能」）である。一方、Ｕｓｅｒｓの場合には、［Ｃ：￥ＤＯＣ￥公開情報］には読み書き自由でアクセス可能（アクセス権の種類：「変更可能」）であるが、［Ｃ：￥ＤＯＣ￥機密事項］にはアクセスすることができない（アクセス権の種類：アクセス不可）。

【００４６】

なお、アクセス権設定テーブル１５はファイルやフォルダだけでなく、プログラムに対してもアクセス権の種類を設定することができる。また、ＵＮＩＸ等のＯＳで使用されるディレクトリであっても、同様に設定可能である。

【００４７】

また、本実施の形態では、アクセス権設定テーブル１５をＯＳの機能により設定入力するとしたが、ＯＳがその設定を参照できるならばアプリケーションにより設定入力するようにしてもよい。

【００４８】

以上の設定に基づき、図５及び図６のフローチャートに沿ってセキュリティ制御の具体例を簡単に説明する。まず、ユーザは、ユーザ名Ｕｓｅｒ１にて自宅で携帯型パーソナルコンピュータ２０に電源を入れ（Ｓ５０）、ＯＳにログインする（Ｓ５１）。ログイン直後、アプリケーションにより、現在位置の検出が行われる（Ｓ５２）。この場合は、［位置の範囲］：Ｈ＜緯度＜Ｉ、Ｇ＜経度＜Ｊ、［ユーザ名］：Ｕｓｅｒ１なので、図３のレコードＮｏ．５に該当する（Ｓ５４、ＹＥＳ）。よって、ユーザはＡｄｍｉｎｉｓｔｒａｔｏｒｓのグループに所属する様に設定される（Ｓ６２）。従って、Ｕｓｅｒ１が［Ｃ：￥ＤＯＣ￥機密事項］及び［Ｃ：￥ＤＯＣ￥公開情報］のフォルダにアクセスしようとした場合（Ｓ６３、ＹＥＳ）、読み書き自由でアクセス可能となる（Ｓ６７）。

【００４９】

次に、ユーザが会社に向かうために移動する場合、ユーザが通勤経路の領域（Ｅ＜緯度＜Ｆ、Ｄ＜経度＜Ｇ）に移動した後に、位置の検出が行われると（Ｓ５２）、この場合は、図３のセキュリティ情報テーブル１４のレコードＮｏ．３に該当するので、ユーザはＵｓｅｒｓのグループに所属する様に設定される（Ｓ６

２）。従って、［Ｃ：￥ＤＯＣ￥公開情報］には読み書き自由でアクセス可能であるが（Ｓ６７）、［Ｃ：￥ＤＯＣ￥機密事項］にはアクセスすることができない（Ｓ６５）。

【００５０】

次に、ユーザが会社の領域：Ａ＜緯度＜Ｂ、Ｃ＜経度＜Ｄに移動した後に、位置の検出が行われると（Ｓ５２）、図３のセキュリティ情報テーブル１４のレコードＮｏ．１に該当するので、ユーザはＡｄｍｉｎｉｓｔｒａｔｏｒｓのグループに所属する様に設定される（Ｓ６２）。従って、［Ｃ：￥ＤＯＣ￥機密事項］及び［Ｃ：￥ＤＯＣ￥公開情報］のフォルダに読み書き自由でアクセス可能となる（Ｓ６７）。

【００５１】

本実施の形態においては管理装置が位置する場所に応じてセキュリティ制御を行っているが、本発明は管理装置と被管理装置が異なる場合にも適用可能である。このような場合には、上述した実施の形態の構成以外に、少なくとも、管理装置と被管理装置間で情報の送受を可能とする構成を必要とすると共に、被管理装置が管理装置からの指示に従って制御を実行する構成を必要とする。このような実施の形態においては次のような構成例となる。

【００５２】

管理装置は位置検出部を備え、その位置検出部は被管理装置自身が検出した位置情報を被管理装置から受信して被管理装置の現在位置を認識する。もしくは位置情報サービスを利用して被管理装置を検索してその現在位置を認識するようにする。

【００５３】

また、被管理装置は、入出力制御部を備え、入出力制御部によりログイン時に入力されたユーザ名を無線通信などにより管理装置に通知し、管理装置はそのユーザ名を無線通信などにより受信する機能を備える。

【００５４】

さらに、管理装置はセキュリティ設定切替え部を備え、被管理装置の現在位置と被管理装置から受信したユーザ名を用いてセキュリティ情報テーブル１４を参

照し、対応する「ユーザの所属するグループ名」を特定し、そのグループ名を被管理装置に通知する。被管理装置においては、管理装置からグループ名を受信してそれを設定し、アクセス権設定テーブル１５に基づいてアクセス制御を行う。

【００５５】

以上、本発明の様々な実施の形態を説明したが、本発明は上述した実施の形態に限定されることはなく、様々な形態のパーソナルコンピュータはもちろんのこと、ワークステーションなどの他種別のコンピュータ、ＰＤＡ（Personal Digital Assistant）などの携帯情報機器、ハンディターミナルなどの専用端末、ゲーム機、携帯電話などの各種装置に技術思想を変更しない範囲で本発明を適用可能であることは言うまでもない。又、上述した実施の形態では、ＯＳ及びＯＳ上で動作するアプリケーションで本発明に係る様々な処理を実行するとしたが、ＯＳのみ、またはアプリケーションのみで本発明の処理を実行する形態であってもよい。

【００５６】

（付記１）所定の装置のセキュリティを管理するセキュリティ管理装置であって、前記所定の装置の位置を検出する位置検出手段と、前記位置検出手段により検出された位置に応じてセキュリティレベルを変更する制御手段とを備えたことを特徴とするセキュリティ管理装置。

（付記２）付記１に記載のセキュリティ管理装置において、セキュリティレベルを位置に対応付けて記憶するセキュリティ情報記憶手段を備え、前記制御手段は前記位置検出手段により検出された位置に基づいて、前記セキュリティ情報記憶手段に記憶されたセキュリティレベルに変更することを特徴とするセキュリティ管理装置。

（付記３）付記２に記載のセキュリティ管理装置において、前記セキュリティレベルはさらにユーザに対応付けられて前記セキュリティ情報記憶手段に記憶され、前記制御手段は前記位置検出手段により検出された位置と前記ユーザとに基づいて、前記セキュリティ情報記憶手段に記憶されたセキュリティレベルに変更することを特徴とするセキュリティ管理装置。

（付記４）付記３に記載のセキュリティ管理装置において、前記ユーザをユーザ

識別子として入力設定することができるログイン機能を備えていることを特徴とするセキュリティ管理装置。

（付記５）付記２乃至付記４のいずれかに記載のセキュリティ管理装置において、

前記セキュリティ情報記憶手段に記憶される情報を入力し、又は前記セキュリティ情報記憶手段に記憶された内容を変更又は削除するためのセキュリティ情報設定手段を備えたことを特徴とするセキュリティ管理装置。

（付記６）付記１乃至付記５のいずれかに記載のセキュリティ管理装置において、前記セキュリティレベルには、前記制御手段によりセキュリティ制御が行われる対象と、その制御内容が規定されていることを特徴とするセキュリティ管理装置。

（付記７）付記６に記載のセキュリティ管理装置において、前記セキュリティ制御が行われる対象は、前記所定の装置が扱うファイルもしくはフォルダもしくはディレクトリもしくはプログラムの少なくともいずれかであることを特徴とするセキュリティ管理装置。

（付記８）付記６又は付記７に記載のセキュリティ管理装置において、前記対象についての制御内容は、アクセス権の種類であることを特徴とするセキュリティ管理装置。

（付記９）付記１乃至付記８のいずれかに記載のセキュリティ管理装置は、前記所定の装置内に設けられていることを特徴とするセキュリティ管理装置。

（付記１０）付記１乃至付記９のいずれかに記載のセキュリティ管理装置において、前記制御手段はＯＳで構成され、前記所定の装置はパーソナルコンピュータであることを特徴とするセキュリティ管理装置。

（付記１１）所定の装置のセキュリティを管理するセキュリティ管理方法であって、前記所定の装置の位置を検出する位置検出ステップと、前記位置検出ステップにより検出された位置に応じてセキュリティレベルを変更する制御ステップとを備えたことを特徴とするセキュリティ管理方法。

（付記１２）所定の装置のセキュリティを管理するセキュリティ管理用プログラムであって、前記所定の装置の位置を検出する位置検出ステップと、前記位置検

出ステップにより検出された位置に応じてセキュリティレベルを変更する制御ステップとをコンピュータに実行させることを特徴とするセキュリティ管理用プログラム。

（付記１３）付記１２に記載のセキュリティ管理用プログラムにおいて、前記制御ステップはＯＳが行うことを特徴とするセキュリティ管理用プログラム。

（付記１４）所定の装置に格納されるプログラムであって、前記所定の装置の位置が検出された場合、予め位置に対応付けられて記憶されたセキュリティレベルを、前記検出された位置に基づいて参照し、前記所定の装置のセキュリティ制御を行うことをコンピュータに実行させるプログラム。

（付記１５）付記１４に記載のプログラムはＯＳであり、ＯＳの機能の一部として前記所定の装置のセキュリティ制御を行うことを特徴とするプログラム。

（付記１６）所定の装置のセキュリティを管理するための処理を実行するためのデータを記憶したコンピュータ読み取り可能なデータ記憶媒体であって、位置とセキュリティレベルが対応付けられて記憶されており、前記セキュリティレベルは、前記所定の装置の検出位置に基づいて参照され、参照結果に基づいて前記所定の装置のセキュリティ制御が行われるための情報であることを特徴とするコンピュータ読み取り可能なデータ記憶媒体。

（付記１７）付記１６に記載のコンピュータ読み取り可能なデータ記憶媒体において、前記記憶された位置とセキュリティレベルは可変であることを特徴とするコンピュータ読み取り可能なデータ記憶媒体。

（付記１８）付記１６又は付記１７に記載のコンピュータ読み取り可能なデータ記憶媒体に記憶された情報に対し、入力もしくは削除もしくは変更を行うセキュリティレベル編集用プログラム。

【００５７】

【発明の効果】

以上説明したように、本発明によれば、特定のエリアでのみ、携帯型パーソナルコンピュータのＯＳの起動やファイルのアクセスを可能とすることができ、また、特定のエリア外に移動した場合は、ＯＳの起動やファイルのアクセスを不可能とすることができる。それによりセキュリティ機能の向上を図ることができる

。つまり、ＯＳへの再ログインを行うことなくセキュリティの設定変更が行われ、その結果、ユーザが誤って、第三者が多い場所（上述の例では通勤経路）にて、機密事項を有するファイルを開いてしまうことによる機密事項の漏洩を防ぐことが可能となる。

【００５８】

また、本発明を利用することにより、例えばパーソナルコンピュータ販売店での万引き防止や、パーソナルコンピュータを貸出してのイベント実施時のパーソナルコンピュータの盗難防止が可能となる。

【図面の簡単な説明】

【図１】

本発明に係る実施の形態におけるセキュリティ管理装置の一実施例のブロック図である。

【図２】

本発明に係る実施の形態におけるセキュリティ管理装置が適用される携帯型パーソナルコンピュータ装置の構成例である。

【図３】

セキュリティ情報テーブルの一例である。

【図４】

アクセス権設定テーブルの一例である。

【図５】

セキュリティ管理のフローチャートである。

【図６】

セキュリティ管理のフローチャートである。

【図７】

電源切断時に表示されるポップアップメッセージの表示例である。

【図８】

アクセス権変更処理時に表示されるポップアップメッセージの表示例である。

【図９】

セキュリティ情報テーブルに対する入力画面例である。

【図１０】

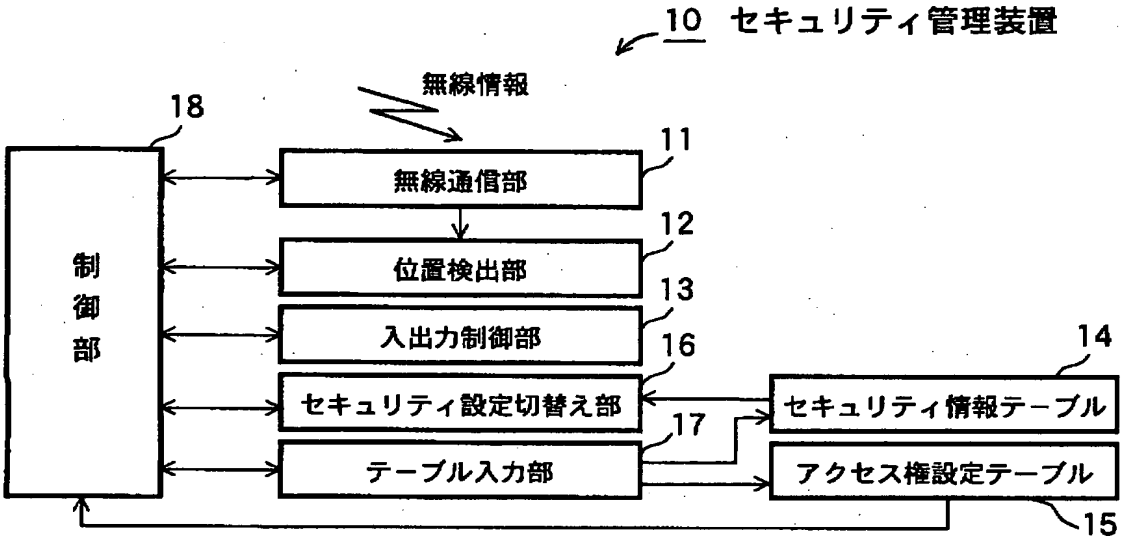
セキュリティ情報テーブルの設定入力画面にて入力される位置範囲（会社、通勤経路、自宅）の経度及び緯度の一例を示した図である。

【符号の説明】

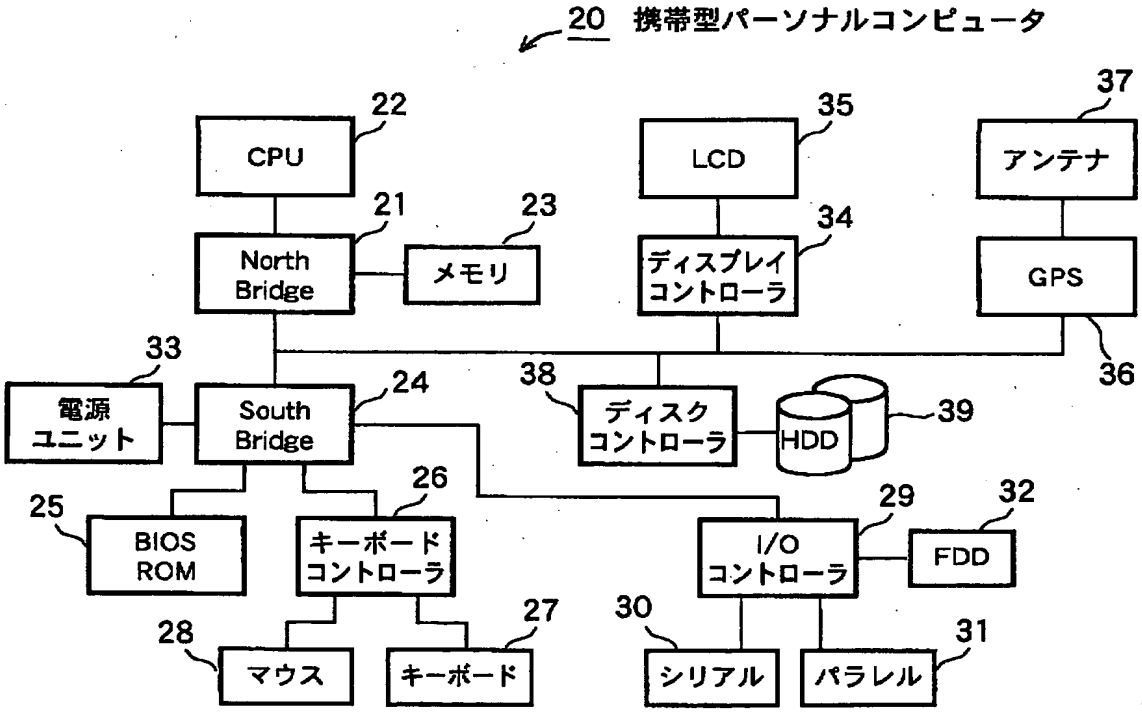
１０　セキュリティ管理装置、１１　無線通信部、１２　位置検出部、１３　入出力制御部、１４　セキュリティ情報テーブル、１５　アクセス権設定テーブル、１６　セキュリティ設定切替え部、１７　テーブル入力部、１８　制御部。

【書類名】　　図面

【図１】


10 セキュリティ管理装置
無線情報
18
制御部
11
無線通信部
12
位置検出部
13
入出力制御部
16
セキュリティ設定切替え部
17
テーブル入力部
14
セキュリティ情報テーブル
アクセス権設定テーブル
15

【図２】


20 携帯型パーソナルコンピュータ
CPU
22
LCD
35
アンテナ
37
North Bridge
21
メモリ
23
ディスプレイコントローラ
34
GPS
36
電源ユニット
33
South Bridge
24
ディスクコントローラ
38
HDD
39
BIOS ROM
25
キーボードコントローラ
26
I/Oコントローラ
29
FDD
32
マウス
28
キーボード
27
シリアル
30
パラレル
31

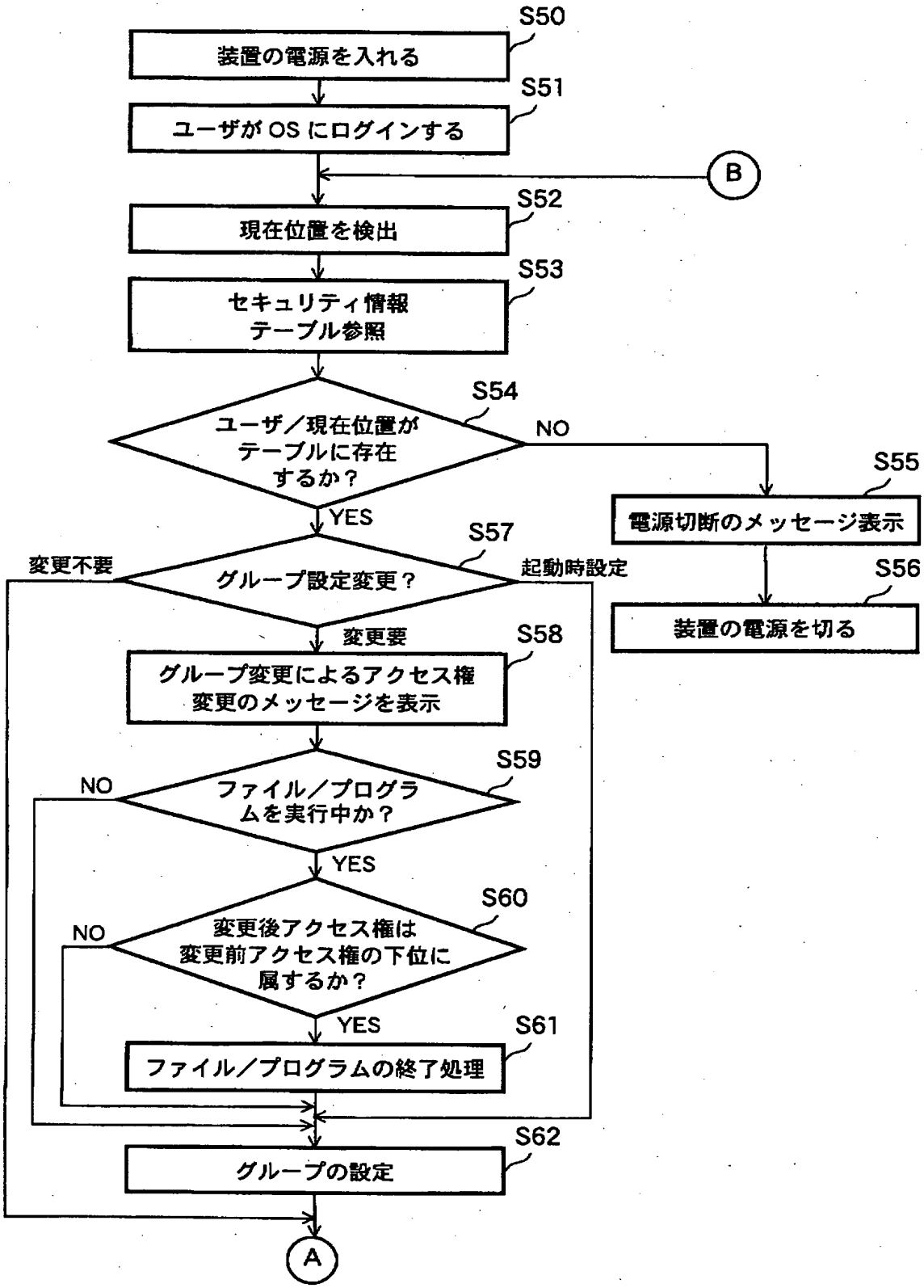
【図３】

レコードNo.	位置の範囲	ユーザ名	ユーザの所属するグループ名
1	A＜緯度＜B、C＜経度＜D	User1	Administrators
2	A＜緯度＜B、C＜経度＜D	User2	Administrators
3	E＜緯度＜F、D＜経度＜G	User1	Users
4	E＜緯度＜F、D＜経度＜G	User2	Users
5	H＜緯度＜I、G＜経度＜J	User1	Administrators
6	H＜緯度＜I、G＜経度＜J	User2	Users
:	:	:	:
:	:	:	:

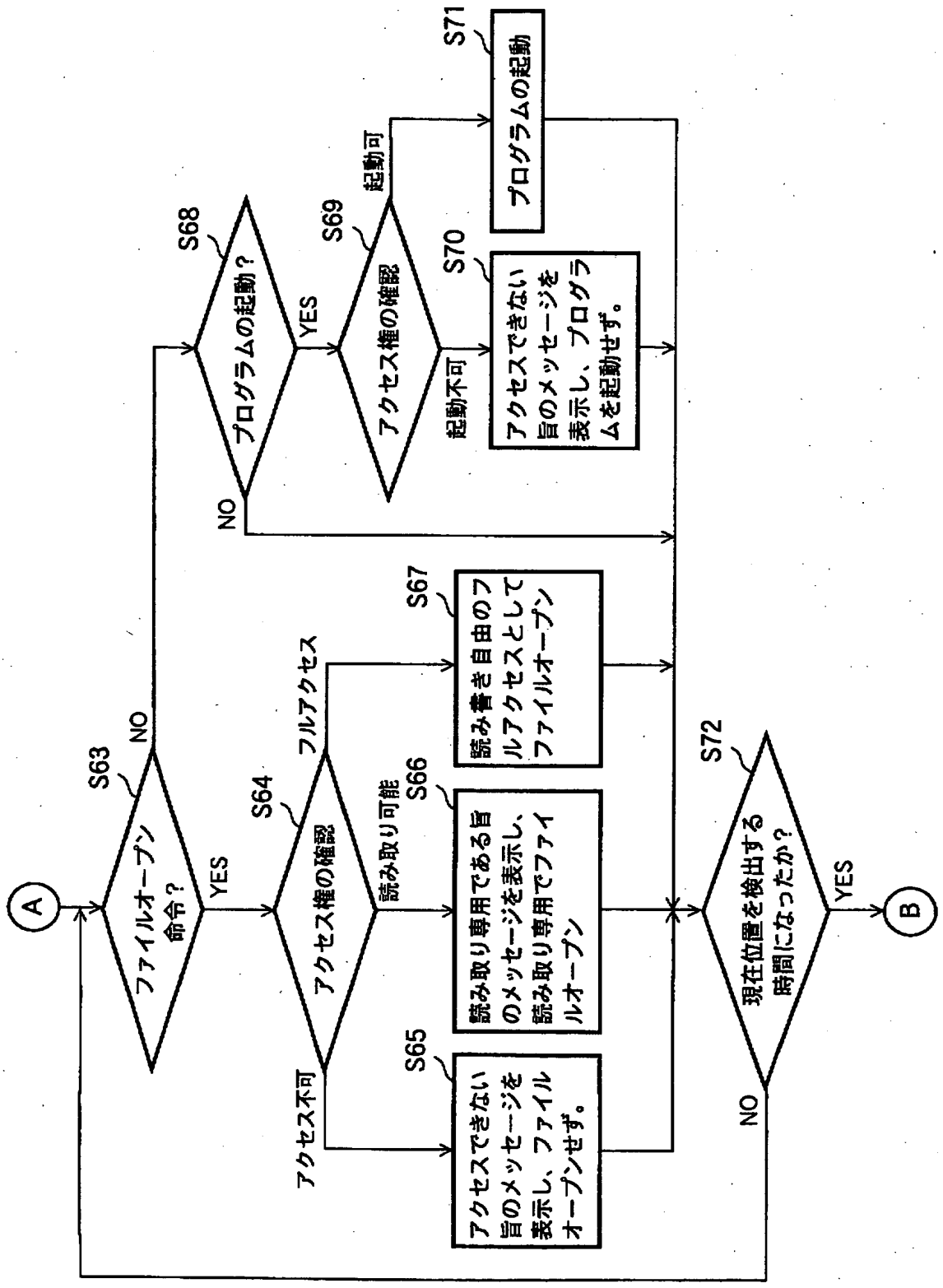
【図４】

ファイル／フォルダ	グループ	アクセス権の種類
C:¥DOC¥機密事項	Administrators	変更可能
	Sub Administrators	読み取り可能
	Users	アクセス不可
	Guests	アクセス不可
C:¥DOC¥公開情報	Administrators	変更可能
	Sub Administrators	変更可能
	Users	変更可能
	Guests	変更可能
:	:	:
:	:	:

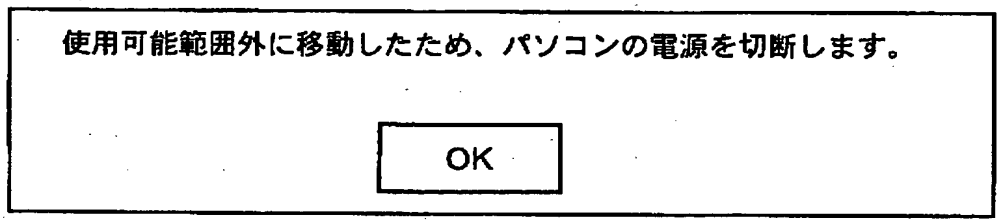
【図５】


S50
装置の電源を入れる
S51
ユーザがOSにログインする
B
S52
現在位置を検出
S53
セキュリティ情報
テーブル参照
S54
ユーザ／現在位置が
テーブルに存在
するか？
NO
S55
電源切断のメッセージ表示
S56
装置の電源を切る
YES
S57
グループ設定変更？
変更不要
起動時設定
変更要
S58
グループ変更によるアクセス権
変更のメッセージを表示
S59
ファイル／プログラ
ムを実行中か？
NO
YES
S60
変更後アクセス権は
変更前アクセス権の下位に
属するか？
NO
YES
S61
ファイル／プログラムの終了処理
S62
グループの設定
A

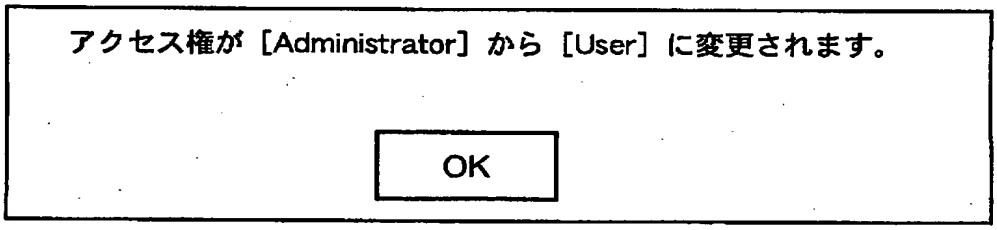
【図６】


A
ファイルオープン命令？
S63
NO
YES
アクセス権の確認
S64
フルアクセス
読み取り可能
アクセス不可
S65
アクセスできない旨のメッセージを表示し、ファイルオープンせず。
S66
読み取り専用である旨のメッセージを表示し、読み取り専用でファイルオープン
S67
読み書き自由のフルアクセスとしてファイルオープン
現在位置を検出する時間になったか？
S72
NO
YES
B
プログラムの起動？
S68
YES
NO
アクセス権の確認
S69
起動可
起動不可
S70
アクセスできない旨のメッセージを表示し、プログラムを起動せず。
S71
プログラムの起動

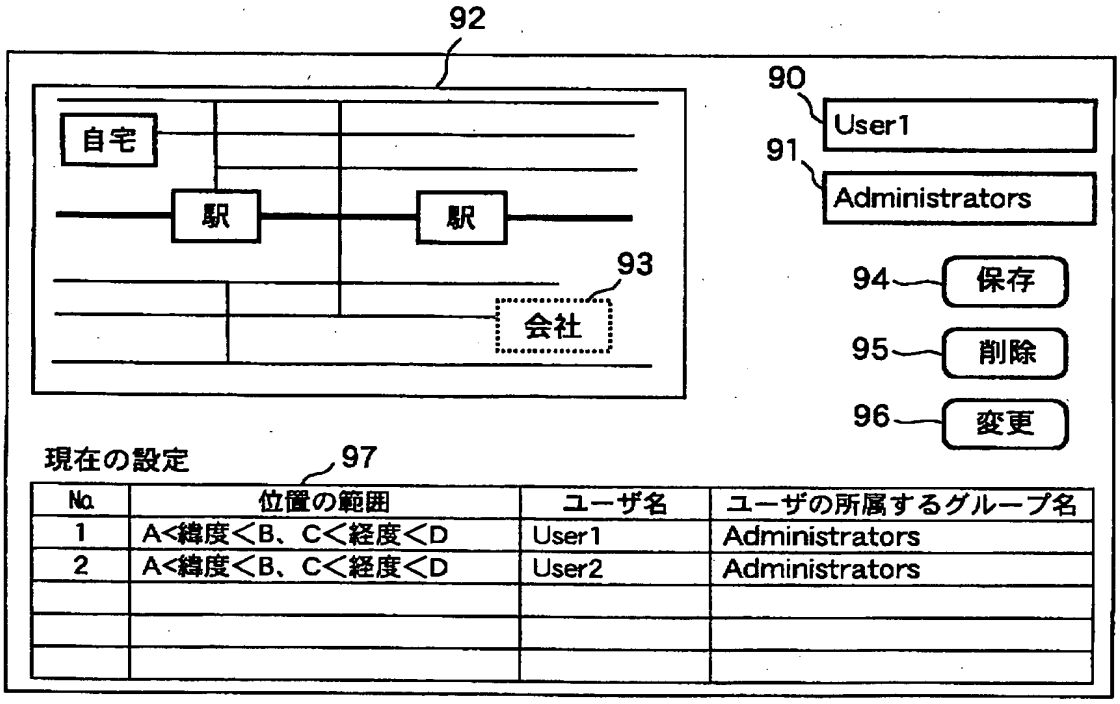
【図７】



【図８】

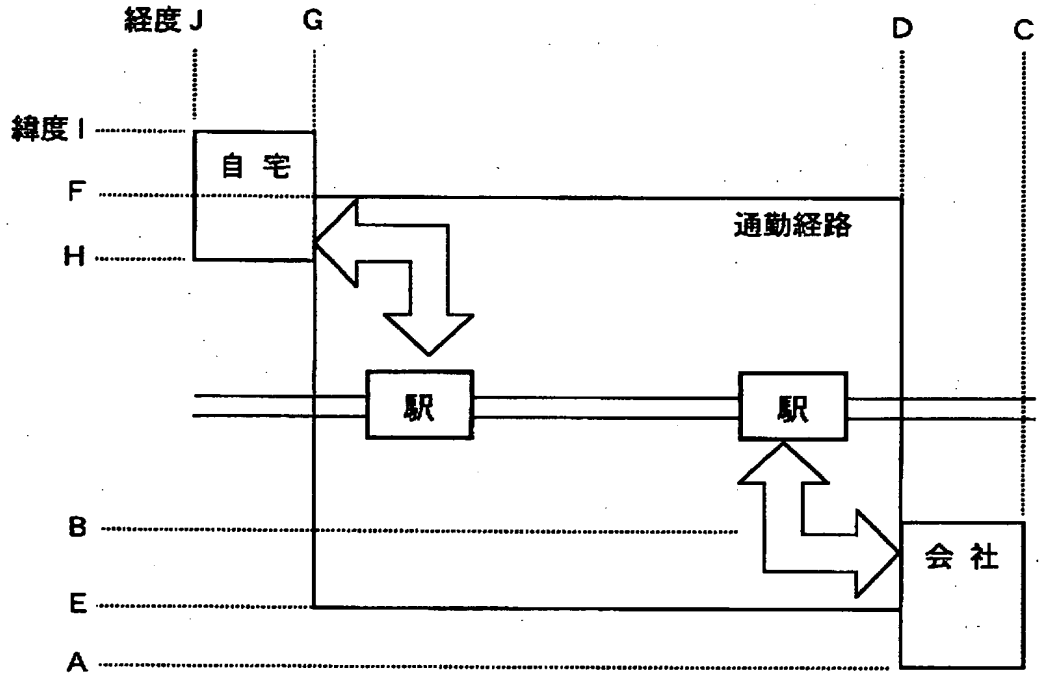


【図９】



No.	位置の範囲	ユーザ名	ユーザの所属するグループ名
1	A<緯度<B、C<経度<D	User1	Administrators
2	A<緯度<B、C<経度<D	User2	Administrators

【図１０】



【書類名】　　要約書

【要約】

【課題】　現在位置に応じてファイルやフォルダ等のアクセス制御を行うセキュリティ管理装置及びセキュリティ管理方法並びにセキュリティ管理用プログラムを提供する。

【解決手段】　携帯端末等のセキュリティ管理を行うにあたり、予めセキュリティレベルを位置に対応付けて所定のテーブルに記憶しておき、ＧＰＳ等により携帯端末の現在位置を検出し、検出した位置に対応したセキュリティレベルを所定のテーブルから取得し、取得したセキュリティレベルに基づいてプログラムの起動やファイル及びフォルダのアクセスの制御を行う。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００１－２９３１３２
受付番号	５０１０１４１４７０５
書類名	特許願
担当官	第七担当上席　０００９６
作成日	平成１３年　９月２７日

＜認定情報・付加情報＞

【提出日】　平成13年 9月26日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社